

STATEMENT OF

LEE COLWELL, DPA

EXECUTIVE DIRECTOR, PEGASUS RESEARCH FOUNDATION

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY,

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING,

AND TERRORISM RISK ASSESSMENT

JULY 20, 2005

Chairman Simmons, Ranking Member Lofgren, and Subcommittee Members:

Thank you for the opportunity to appear before this Committee and provide you with information and my views about law enforcement and homeland security information sharing, especially regarding the needs of local agencies for Local-To-Local (L2L) law enforcement data communications, not voice (i.e., public safety radio). I speak especially to the needs of agencies in rural and small-town America. Thank you also for the work you do to make all our communities and Nation safer places for all Americans.

My name is Lee Colwell. I am Executive Director of the Pegasus Research Foundation, located in Little Rock, AR. I am a Former Associate Director of the FBI, the number two position in the FBI at the time, a retired university professor, a life member of the NSA and IACP. My entire professional career has been deeply involved in law enforcement and public safety at all levels of government.

I am speaking on the need for L2L data communications, especially in rural areas, on behalf of the Pegasus Program, which includes Pegasus Technology Consortium members from Colorado, Iowa, Kentucky, Minnesota, Mississippi, Pennsylvania, and Virginia. I will discuss what the Pegasus program is, what Pegasus is not, what the program does, the background on local law enforcement, how Pegasus could assist the Department of Homeland Security, and a final comment on information sharing.

I also reflect the views, I believe, of the approximately 700 local law enforcement agencies from more than 30 states, from Maine to California and Washington to Florida, and numerous points in between, which Pegasus currently serves, either by providing an outlet for their local agency legacy data, or by providing access to that data which is not available elsewhere, or both. A map showing the location of those local agencies involved in the Pegasus Program is attached to my written statement.

WHAT THE PEGASUS PROGRAM IS

The Pegasus program is Congressionally-led. Pegasus is locally managed as a nationwide initiative for highly-secure nationwide L2L legacy data exchange of local law enforcement and homeland security data. As far as we know, the Congressionally initiated Pegasus program is the only nationwide program with a strategy and plan for nationwide implementation.

Pegasus is a good example of how Congress provided for previously unmet local agency needs to solve an essentially Federal problem by engaging thousands of local front line law enforcement personnel in the solution. Pegasus was initiated by the National Sheriffs' Association in 2000 and supported by Congress in 2001 prior to 9/11.

With continued support, Pegasus provides a basic tool that serves local agency needs for L2L law enforcement data communications. This is especially critical to those small and rural agencies where the need is the greatest because they have limited or few financial and information technology resources and little or no access to local agency data from other areas.

The Pegasus Program has been working with local agencies to build local agency consensus on local agency data sharing, namely:

- a) what information do local agencies want to share;
- b) how do they want to share it; and,
- c) who do they want to share it with.

Based on needs assessment work over several years and on-going policy guidance of local law enforcement, the Pegasus Program has implemented a technology solution that reflects the “bottom-up” needs of local agency. This program is designed to provide access to specific and actionable local law enforcement information on a real-time or near-real-time basis, and the ability to communicate that data without human intervention.

During the first half of 2005, more than 750 county Sheriff’s Offices and municipal police departments in more than 30 states participated in the Pegasus Program, either by contributing data, accessing data, or both. Pegasus is providing authorized secure access to local law enforcement booking and warrant data that is nowhere else available, and has taken first steps to provide access to local incident data nowhere else available. This has been achieved in a little over a year, with fairly nominal levels of Federal funding, and is poised to rapidly expand with additional funding.

Built around secure encrypted Internet transport and the Department of Justice Global Justice XML Data Model and other Federal standards wherever possible, Pegasus uses commercial off-the-shelf (COTS) technology. The data is highly-secure, in particular through biometric fingerprint access authentication. This process is implemented through formal enrollment procedures and fingerprint-based authentication technology that is more resistant to “hacking” than commonly used UserID/Password systems. This authentication technology allows system administrators to “track the insider”, which is perhaps the greatest security risk. To do this Pegasus uses COTS fingerprint readers that are marketed by a dozen different manufacturers and COTS software.

Pegasus is a highly cost-effective vehicle for regional information sharing projects, especially for local agencies in small towns and rural areas that do not have the financial and information technology resources to build technology-intensive data sharing capabilities. A good example here is the rural law enforcement agencies in Virginia, West Virginia and Maryland located near Clarke County, Virginia which work with the Mount Weather Police Department to provide security to FEMA facilities in the area. These local agencies want and need a secure information exchange capability of the type that can be provided both by and to the Mount Weather PD. Pegasus has been working with them with the view toward providing that capability.

The Pegasus program builds on existing technology deployment which significantly reduces time to deploy, training, capital and implementation costs, and maintenance costs. This has the added benefit of making it fast and cheap to deploy relative to other “common software” and “common data center” initiatives.

Your colleagues in the Senate have recently made it clear that improved information sharing among emergency responders is essential to a comprehensive homeland security response. Improved information sharing among emergency responders is also essential to homeland security preparedness, as well as homeland response.

A classic “dual-benefit” system, Pegasus is primarily focused on local agency needs, starting with local law enforcement, but also can serve Federal law enforcement and Homeland Security by making local agency data available for Federal personnel access, not extraction, in accordance with local agency policies. Pegasus is working with several federal law enforcement agencies to help them achieve their law enforcement information exchange mission on terms acceptable to local law enforcement.

WHAT PEGASUS IS NOT

Pegasus is not a theoretical or “ivory tower” standards-setting body. Pegasus does advance and implement Federal standards like the Global Justice XML Data Model, which have been adopted by DHS. Most importantly, Pegasus is actually working in the field to implement Federal standards, not just discuss them.

Pegasus does not replicate what is in place—where a regional information sharing system is in place which meets Pegasus security and other policy requirements, Pegasus works with those system’s to provide a conduit for data to be exchanged in and out of the region.

Pegasus does provide a nationwide, Internet based conduit by which local agency information in these regional systems can be accessed nationally, and by which local agency information outside these regions may be accessed by these regional systems, subject to meeting Pegasus security standards, in particular biometric access authentication.

Many regional systems do not use biometrics or other strong access authentication technologies and processes—and we are unable to share with them because the Pegasus governing policy is to share only with systems that have biometric fingerprint access authentication technologies and processes in place.

In this connection, Pegasus is working with local law enforcement agencies in several locations that have adopted the biometric fingerprint access authentication technologies and processes. These include agencies in Hinds, Madison and Rankin Counties, Mississippi; Jefferson County, Alabama and surrounding counties along Interstate 20; Marshall County, Iowa and surrounding counties; Linn County, Iowa and its police departments; Calhoun County, Michigan and surrounding counties; the Vermont Sheriffs’ Association; and, the County Sheriffs of Colorado. Pegasus provides cost-effective services to these regional information exchange efforts. A point of discussion is that most local information sharing systems are being built without strong access authentication technologies. As a result, Pegasus security policies do not allow their linkage.

Pegasus is not a data aggregator that owns local agency data, but a data utility that transports local agency data. Unlike some other initiatives, Pegasus does not push privacy boundaries or mix law enforcement and private sector data in powerful data mining technologies. Pegasus focuses on enabling traditional exchange of law enforcement data. The Pegasus program emphasis is on information exchange of traditionally collected law enforcement data and automating those processes.

WHAT THE PEGASUS PROGRAM DOES

Pegasus' mission is to serve as a nationwide vehicle for local law enforcement and public safety data in existing legacy systems to be securely accessed (but not extracted) by authorized law enforcement, public safety and Homeland Security users at all levels of government, within policy and security framework approved at the local agency level.

Pegasus builds local agency consensus and speaks for local-level agencies nationwide on data integration and data interoperability issues. It provides a nationwide L2L biometric fingerprint-secured law enforcement data communications service for agencies located in both rural and urban areas, ranging from Dawes County, Nebraska, with a population of 9,060, to Los Angeles County, California, with a population of over 9,800,000.

Pegasus provides legacy database integration for local law enforcement agencies nationwide. This system can facilitate law enforcement agencies at local as well as State and Federal levels to access but not extract legacy data that local agencies wish to share. The program also provides a nationwide directory of critical contact information useful to local agencies; secure messaging and alerting capabilities that represent a secure alternative to inherently insecure email; services that automate exchange of information by local law enforcement, such as consular notifications of foreign nationals who have been arrested or detained; shared mapping for local agency location and local critical infrastructure location; and, training on data interoperability issues.

The Pegasus program governance is through the Pegasus Advisory Board. Our policy board consists of sitting or recently-retired local law enforcement officials. The Pegasus Advisory Board addresses nationwide local-level agency policy on data interoperability issues as they are developed.

BACKGROUND ON LOCAL AGENCIES AND LOCAL LAW ENFORCEMENT

As you know, under our Federal system of Government, the overwhelming majority of law enforcement activity is carried out by local law enforcement—some 14,000 local law enforcement agencies composed of approximately 3,100 Sheriff's Offices, led by Sheriffs who are typically the highest constitutionally-elected officials in most counties, and about 11,000 municipal police departments.

There are some 160 large U.S. cities and counties, served by a few hundred large local law enforcement agencies—Sheriff's Offices and Police Departments—that provide law enforcement and public safety services to the majority of the Nation's population living and working in a small fraction of the Nation's landmass.

These urban areas and their law enforcement agencies serving them face many challenges. When compared to non-urban law enforcement these large urban areas have significant resource advantages; e.g., access to personnel with cutting edge technology expertise, large tax bases with significant tax revenues, and the specially-focused Federal programs such as the Homeland Security Urban Area Security Initiative (UASI), which focuses on the needs of the largest urban areas.

At the same time, a very significant portion of the Nation's population and the critical infrastructure serving the entire nation, including bridges and dams, interstate transportation network, railroads, shipping, chemical plants, pipelines, nuclear and conventional power plants and electric transmission facilities, are located in predominantly rural counties. These rural areas are served by more than 13,000 local law enforcement agencies—the vast majority of law enforcement agencies. These small police departments and Sheriff's Offices typically have 5 or less employees, and are located in small non-urban communities with a static at best or declining tax bases: 89.7% of local law enforcement agencies serve populations of less than 25,000. These municipal police departments and Sheriffs offices serving rural and small town America are a special focus area for the Pegasus Program.

The Pegasus Program was conceived of by the Nation's Sheriffs in the Spring of 2000, to address their need to make their data available to their local law enforcement partners, in "local-to-local communication". As you know, 90% of the deputy sheriffs work for an office with a jail and as such, these offices are the primary source of information about persons arrested and detained for illegal actions, including criminal aliens. Sheriffs and municipal police departments work together daily on criminal investigations and other routine law enforcement matters which require secure L2L data communications capabilities. This kind of L2L communications is behind the explosive deployment of regional information sharing projects around the Nation, many of them "regional stovepipes" which do not have L2L communications capabilities outside their small region.

Rural and small local agencies do not operate in isolation nor are they immune from the crime in the rest of the Nation. Historically, every major US terrorist incident has involved major direct contact with rural law enforcement—ranging from the 9/11 hijackers to the Unabomber, to the Midwest Pipe Bomber to Timothy McVeigh to Eric Robert Rudolph, the 1996 Atlanta Olympic Games Bomber. Currently, two of our Nation's more significant law enforcement challenges—methamphetamine and gang activity—heavily involve urban/rural interaction. Most methamphetamine production in the Nation takes place in rural America, where it can be produced without detection before being transported to both urban and rural areas. Similarly, gang activity, a traditionally-urban phenomenon, is spreading from urban areas to rural areas throughout the Nation. Because criminal gangs from Central America, in particular, are "franchising" rural areas, the Nation's local law enforcement leadership in large urban areas, such as Los Angeles Sheriff's Department, are seeking ways to work more effectively with rural law enforcement to control the gang problem, and are looking to Pegasus and other vehicles to help solve our gang problem.

There is a great deal of misunderstanding about where local law enforcement data may be found. It is well understood that most law enforcement activity takes place at the local agency level, and that most law enforcement data is generated and may be found at the local agency where it is generated. The twelve million plus reported crimes by the Uniform Crime Report data are crimes in local jurisdictions. Many Federal policymakers and agencies also perceive that the National Crime Information Center (NCIC) or the State agencies generally known as the "State Crime Information Centers" have access to all of this local law enforcement data: in fact, nothing could be further from the truth. All narrative criminal offense/incident reports and most misdemeanor warrants are created and reside exclusively at the municipal and county level—not at the State level. These records contain specific and actionable information of great value to

law enforcement at all levels of government, but, in my opinion, the vast majority of them will never be accessible by local, State or Federal law enforcement except through L2L data exchange of the kind that Pegasus is providing.

Enormous quantities of specific and actionable law enforcement data—highly useful to persons with law enforcement and homeland defense responsibilities at local, State and Federal levels of government. These records remain within local agencies and local agency computer systems, and are never accessed by other agencies. It is estimated 80-90% of local agency warrants are not reflected in the NCIC or State Crime Information Centers. These records not in NCIC are primarily misdemeanor and some felony warrants (most frequently due to costs to extradite). This data represents a tremendous potential resource for the Nation's homeland security and other Federal law enforcement agencies.

There is also a major policy issue regarding Federal access to local law enforcement data, as opposed to unfettered Federal extraction of local agency data to reside in Federal databases for manipulation by Federal agencies. Federal access to local agency data is generally supported by local law enforcement, but local law enforcement data is solidly opposed to Federal extraction of their data, which raises numerous privacy and legal issues. In this connection, 42 USC § 3789d, "Prohibition of Federal control over State and local criminal justice agencies", provides in relevant part as follows: "(a) Nothing in this chapter or any other Act shall be construed to authorize any department, agency, officer, or employee of the United States to exercise any direction, supervision, or control over any police force or any other criminal justice agency of any State or any political subdivision thereof."

The overwhelming view of local agency officials nationwide is that Federal extraction of local law enforcement data is a significant start down the slippery slope to prohibited Federal control over local police. The overwhelming majority of local law enforcement leaders are prepared to allow Federal agencies to access their data on local agency terms, but are not about to start down the slippery slope toward Federal control over local policing, which is inherent in Federal extraction of local agency data.

I will now address the ambiguous usages of the term "information sharing", which means different things to different users. Most Federal information sharing initiatives are driven by Federal needs and perspectives. For most Federal information sharing initiatives, "information sharing" means providing Federal information from one Federal agency to another Federal agency or pushing Federal data down to a local or State agency. Sometimes it also means providing the capability for local agency to push information up to a State or Federal user.

As important and valid as this Federal view of "information sharing" is, local law enforcement agencies are mostly concerned about a very different type of L2L "information sharing": sharing law enforcement and public safety information with other agencies—mostly municipal police departments and Sheriff's Offices—with which they work on routine criminal investigative matters, some percentage of which carry Federal law enforcement and Homeland Security implications. This is the area of "information sharing" with which local law enforcement and Pegasus are most concerned. Except for Pegasus, we are not aware of any Federal or, for that matter, any non-Federal initiative which has a strategy and plan for nationwide L2L "information sharing."

HOW COULD PEGASUS ASSIST THE DEPARTMENT OF HOMELAND SECURITY IN ACHIEVING ITS MISSIONS?

We believe there are several opportunities.

1) One is The Homeland Security Information Network (HSIN), which serves as a nationwide vehicle for Federal Sensitive But Unclassified (SBU) data to be securely accessed by emergency responders and critical infrastructure sector users. This process occurs within policy and security framework approved by the Federal Government. We believe Pegasus can help with this mission.

2) The ICE Detention and Removal Office (DRO) and other DHS units have information which would be useful for a broad range of law enforcement personnel to have access to, including persons that DHS or local officials may not want to have access to HSIN—e.g., DRO data on alien criminals.

Pegasus and HSIN staffers have discussed working together so that HSIN recognizes Pegasus-authenticated users. That means that Pegasus authenticated users will have credentials and permissions recognized by HSIN. Under this arrangement, Pegasus will bring to HSIN several thousand users in more than 30 states, many of them from rural counties and small agencies are added on to the HSIN first-priority areas. We anticipate that, should HSIN implement strong access authentication with biometrics for law enforcement personnel, Pegasus will recognize the HSIN credentials and permissions of HSIN users, as part of the HSIN Law Enforcement Community.

OTHER INFORMATION SHARING

3) Pegasus is actively facilitating the sharing of relevant and timely information between local law enforcement agencies in its L2L program. Pegasus has also briefed DHS investigative personnel who have indicated a strong interest in having access to a pilot project which would provide sophisticated and link analysis to data maintained in local databases along our southern borders. Pegasus has briefed a number of Department of Justice federal law enforcement agencies including the FBI and DEA and proposed providing access to local data especially jail records. We see relevance to this data with a pilot project and partnership of federal agencies with Pegasus in providing link analysis of these records. We have proposed partnerships with a pilot project utilizing federal prison records with several federal agencies including the FBI, DEA, ICE and DRO.

4) Law enforcement officials at the local level are also concerned about criminal enterprises, including terrorist activity being run from not only the federal prison population but the 3000+ local jails. To investigate such criminal enterprises, authorized investigators (both federal and local) face a daunting and time-consuming process of assembling jail booking records and detail call records. The Pegasus Program with its Pegasus Technology Consortium, believe this existing tool (link analysis) needs to be demonstrated through the pilot projects we have proposed to the above cited agencies.

Mr. Chairman, thank you and all the committee members for allowing me to provide my views on L2L information sharing. We look forward to facilitating a growing dialogue between the

Congress and local agencies, as Congress works to address national law enforcement and Homeland Security needs and the role and needs of local agencies for L2L data communications in that larger context.

I will address any questions you may have.

Pegasus Agency Map

June 2005

KEY

- Accessing Agencies
- Contributing and Accessing Agencies
- Contributing Agencies

